CNCERT/CC

GUIDE FOR PREVENTING RANSOMWARE ATTACKS

Ransomware is a form of malware used by hackers to extort users by hijacking their assets or resources. Hackers can encrypt users' data and change configurations to make their assets or resources inaccessible, and then demand ransom from users in exchange for decryption key or system restoration upon payment. The main forms of extortion include encrypting files, locking screens or systems, and posing data disclosure threats. Ransomware mainly spreads through phishing emails, malware-hosting websites, vulnerabilities, remote intrusion, supply chain and mobile devices.

As indicated in the 2020 Overview of China's Internet Security Landscape recently released by CNCERT, ransomware continued to grow with more than 781,000 cases being detected in 2020, a 6.8% increase compared to 2019. The first half of 2021 has witnessed a series of major ransomware attacks. For example, on March 20, a Taiwan-based computer manufacturer - Acer - suffered a REvil ransomware attack, which was demanded to pay $50 million; on May 7, Colonial Pipeline, an American oil pipeline company, was hit by Darkside, a major ransomware attack, causing shutdown of liquid fuel operations across the east coast of the U.S.; on May 26, a large Chinese real estate company's 3TB of data was stolen and encrypted by REvil ransomware and on May 31, the same ransomware attacked the world's largest meat supplier JBS, leading to suspension of all its meat production in Australia.

9 DOS FOR PREVENTING RANSOMWARE ATTACKS

1 Check your assets and implement hierarchical classification management.

2 Back up important data and systems.

3 Set strong passwords and keep them confidential.

4 Perform regular risk assessment.

5 Run virus scans and disable unnecessary ports regularly.

6 Initiate rigorous identity authentication and access control.

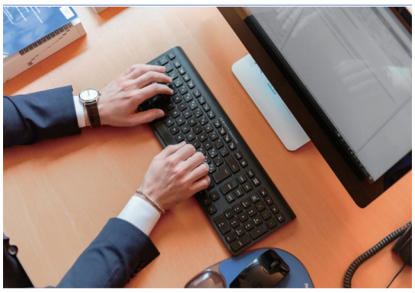
7 Adopt stringent access control strategies.

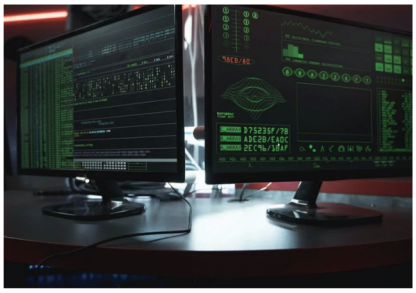
8 Raise cybersecurity awareness.

9 Formulate emergency response plans.

1. Check your assets and implement hierarchical classification management. Check and manage all the information systems and applications within your organization to establish a comprehensive list of assets; sort out the data flow direction among information systems and devices to find out potential routes of attackers' lateral movements; identify the connection between internal systems and external third-party systems, especially the areas where the control is shared with partners, to reduce the risk of ransomware from third-party systems; and classify information systems and data to identify key businesses and systems, the dependent relationships between them and prioritize emergency response actions.

2. Back up important data and systems. Important files, data and service systems should be backed up on a regular basis. Isolation measures should be adopted to restrict access to backup devices and data to prevent lateral movement of ransomware from encrypting backup data.





3. Set strong passwords and keep them confidential. Use strong and random login passwords that contain numbers, upper- and lower-case letters and symbols with a minimum length of at least 8 characters, and change them frequently; and avoid using same passwords on multiple devices within the same LAN, or passwords that are strongly correlated with device information (e.g., IP or device names).

4. Perform regular risk assessment. Carry out risk assessments and penetration tests on a regular basis; identify and document asset vulnerabilities, determine system attack surfaces and promptly patch up security vulnerabilities.

5. Run virus scans and disable unnecessary ports regularly. Install anti-virus software, update virus databases and perform full virus scans in a regular manner; and disable unnecessary services and ports, including unnecessary remote access services (ports 3389 and 22) and shared LAN ports like 135, 139 and 445.

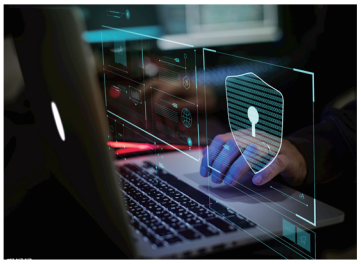
6. Initiate rigorous identity authentication and access control. Strengthen the issuance, management, authentication, cancellation and audit of access credentials to prevent ransomware from illegal obtainment and utilization. It is recommended that a 2-factor authentication approach should be used. Access control should be refined, and the least privilege and responsibility separation principles should be observed to reasonably assign access permissions and authorizations. Standard user accounts, instead of those of administrators, should be used whenever possible.

7. Adopt stringent access control strategies. Strengthen network isolation. Use network segmentation and partitioning technologies to fulfill network isolation across different information devices. Prohibit or restrict unnecessary access channels between different machines within a network. Tighten the management over remote access and restrict access to important data or systems. Disable all unnecessary remote management ports; if the ports must be enabled, use the whitelist policy together with access control technologies such as firewalls, identity authentication and behavior auditing to refine the scope of access permission. Review access control policy on a regular basis.

8. Raise cybersecurity awareness. Provide cybersecurity awareness education for your employees and partners; and educate developers that development and test environments should be isolated from the production environment to prevent the spread of ransomware from the former to the latter.

9. Formulate emergency response plans. Formulate ransomware emergency response plans for important information systems, identify emergency response personnel and their responsibilities, determine emergency response and restoration plans for information systems, and carry out drills regularly. Develop incident response procedures, solicit assistance from cybersecurity companies when necessary to conduct intrusion analysis, and promptly patch up vulnerabilities.

TO PREVENT RANSOMWARE, DON'T DO THE FOLLOWING



1. Don't click on suspicious email links.

Ransomware attackers often take advantage of hot topics that victims are concerned about or even hack into the email accounts of the victim's organization or contacts to send phishing emails. Don't click on links or attachments in these emails. If you receive suspicious emails from your organization or contacts, call them directly to verify.

2. Don't open websites from unreliable sources.

Don't browse websites containing pornographic, gambling and other inappropriate information as these sites are often leveraged by ransomware attackers to launch malware or phishing attacks.

3. Don't install software from unreliable sources.

Don't download or install software from unknown websites or strangers. Be vigilant that ransomware may disguise as an update of regular software.

4. Don't use storage devices from unknown resources.

Don't connect your devices with USB disks, portable hard disks or flashcards from unknown sources.

RANSOMWARE EMERGENCY RESPONSE APPROACHES

When a device is infected with ransomware, don't panic; you can immediately follow the procedures listed below to reduce potential harms.

1. Network isolation. Cut off the connection of infected devices by unplugging the cable or disabling the network connection to avoid further infection of and penetration to other devices.

2. Targeted handling. When important files are found not being encrypted yet, immediately terminate the ransomware process or shut down the device to prevent further losses. However, when you find that all important files have already been encrypted, keep the device as it is and solicit professional assistance.

3. Timely reporting. Timely report to network administrators and inform all potential victims. When serious impacts have been caused, timely report to cybersecurity authorities.

4. Screening and repairing. If necessary, immediately cut off unnecessary connections between machines within the network, and change weak passwords thereof. Conduct comprehensive screening of the intrusion routes and patch up vulnerabilities in time. Perform a comprehensive vulnerability scan and security reinforcement on machines within the network as soon as possible.

5. Professional recovery. Hire cybersecurity companies and professionals to recover data and systems.